Security Limitations of Classical-Client Delegated Quantum Computing

Security Limitations of Classical-Client Delegated Quantum Computing

Christian Badertscher[1], Alexandru Cojocaru[2], Léo Colisson[3](✉), Elham Kashefi[2,3], Dominik Leichtle[3], Atul Mantri[4], Petros Wallden[2]

[1] IOHK, Zurich, Switzerland
christian.badertscher@iohk.io
[2] School of Informatics, University of Edinburgh,
10 Crichton Street, Edinburgh EH8 9AB, UK
ekashefi@inf.ed.ac.uk, a.d.cojocaru@sms.ed.ac.uk, petros.wallden@ed.ac.uk
[3] Laboratoire d'Informatique de Paris 6 (LIP6), Sorbonne Université,
4 Place Jussieu, 75252 Paris CEDEX 05, France
leo.colisson@lip6.fr, dominik.leichtle@lip6.fr
[4] Joint Center for Quantum Information and Computer Science (QuICS),
University of Maryland, College Park, USA
amantri@umd.edu

Abstract. Secure delegated quantum computing allows a computationally weak client to outsource an arbitrary quantum computation to an untrusted quantum server in a privacy-preserving manner. One of the promising candidates to achieve classical delegation of quantum computation is classical-client remote state preparation ($\mathsf{RSP}_{\mathsf{CC}}$), where a client remotely prepares a quantum state using a classical channel. However, the privacy loss incurred by employing $\mathsf{RSP}_{\mathsf{CC}}$ as a sub-module is unclear. In this work, we investigate this question using the Constructive Cryptography framework by Maurer and Renner [MR11]. We first identify the goal of $\mathsf{RSP}_{\mathsf{CC}}$ as the construction of ideal RSP resources from classical channels and then reveal the security limitations of using $\mathsf{RSP}_{\mathsf{CC}}$. First, we uncover a fundamental relationship between constructing ideal RSP resources (from classical channels) and the task of cloning quantum states. Any classically constructed ideal RSP resource must leak to the server the full classical description (possibly in an encoded form) of the generated quantum state, even if we target computational security only. As a consequence, we find that the realization of common RSP resources, without weakening their guarantees drastically, is impossible due to the no-cloning theorem. Second, the above result does not rule out that a specific $\mathsf{RSP}_{\mathsf{CC}}$ protocol can replace the quantum channel at least in some contexts, such as the Universal Blind Quantum Computing (UBQC) protocol of Broadbent et al. [BFK09]. However, we show that the resulting UBQC protocol cannot maintain its proven composable security as soon as $\mathsf{RSP}_{\mathsf{CC}}$ is used as a subroutine. Third, we show that replacing the quantum channel of the above UBQC protocol by the $\mathsf{RSP}_{\mathsf{CC}}$ protocol QFactory of Cojocaru et al. [CCKW19] preserves the weaker, game-based, security of UBQC.

Keywords: Remote State Preparation, Blind Quantum Computing

1 Introduction

The expected rapid advances in quantum technologies in the decades to come are likely to further disrupt the field of computing. To fully realize the technological potential, remote access, and manipulation of data must offer strong privacy and integrity guarantees and currently available quantum cloud platform designs have still a lot of room for improvement.

There is a large body of research that exploits the client-server setting defined in [Chi05] to offer different functionalities, including secure delegated quantum computation [BFK09, MF13, DFPR14, Bro15a, Mah18a, Fit17], verifiable delegated quantum computation [ABOE08, RUV12, FK17, HM15, Bro15b, FHM18, TMM+18, Mah18b, GKK19, Vid20], secure multiparty quantum computation [KP17, KMW17, KW17], and quantum fully homomorphic encryption [BJ15, DSS16]. It turns out that one of the central building blocks for most of these protocols is secure *remote state preparation* (RSP) that was first defined in [DKL12]. At a high level, RSP resources enable a client to remotely prepare a quantum state on the server side and are, therefore, the natural candidate to replace quantum channel resources in a modular fashion. These resources further appear to enable a large ecosystem of composable protocols [DKL12, DFPR14], including in particular the *Universal Blind Quantum Computation* (UBQC) [BFK09] protocol used to delegate a computation to a remote quantum server who has no knowledge of the ongoing computation.

However, in most of the above-mentioned works, the users and providers do have access to quantum resources to achieve their goals, in particular to quantum channels in addition to classical communication channels. This might prove to be challenging for some quantum devices, e.g. those with superconducting qubits, and in general, it also restricts the use of these quantum cloud services to users with suitable quantum technology.

Motivated by these practical constraints, [CCKW18] introduced a protocol mimicking this remote state preparation resource over a purely *classical* channel (under the assumption that the learning-with-error (LWE) problem is computationally hard for quantum servers). This is a cryptographic primitive between a fully classical client and a server (with a quantum computer). By the end of the interactive protocol the client has "prepared" remotely on the server's lab, a quantum state (typically a single qubit $|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$). This protocol further enjoys some important privacy guarantees concerning the prepared state. The important role of such a classical RSP primitive as part of larger protocols – most notably in their role in replacing quantum channels between client and server – stems from their ability to make the aforementioned protocols available to classical users, in particular clients without quantum-capable infrastructure on their end. It is therefore of utmost importance to develop an understanding of this primitive, notably its security guarantees when composed in larger contexts such as in [GV19].

In this paper, we initiate the study of analyzing classical remote state-preparation from first principles. We thereby follow the Constructive Cryptography (CC) framework [MR11, Mau11] to provide a clean treatment of the

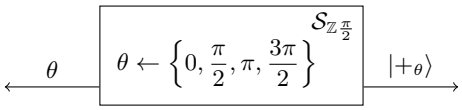


Fig. 1: Ideal resource $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$

RSP primitive from a composable perspective. (Note that the framework is also referred to as Abstract Cryptography (AC) in earlier works.) Armed with such a definition, we then investigate the limitations and possibilities of using classical RSP both in general and in more specific contexts.

1.1 Overview of our Contributions

In this work, we cover the security of $\mathsf{RSP}_{\mathsf{CC}}$, the class of remote state preparation protocols which only use a classical channel, and the use-case that corresponds to its arguably most important application: Universal Blind Quantum Computing (UBQC) protocols with a completely classical client. The UBQC protocol can be divided in two stages: first, the client needs to send random $|+_\theta\rangle$ (with $\theta \in \{0, \frac{\pi}{4}, \ldots, \frac{7\pi}{4}\}$) to the server, and after this initial quantum interaction, the communication is purely classical. In this work, we analyze the security of $\mathsf{UBQC}_{\mathsf{CC}}$, the family of protocols where a protocol in $\mathsf{RSP}_{\mathsf{CC}}$ is used to replace the initial quantum interaction from the original quantum-client UBQC protocol. An example of an RSP resource is the $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$ resource where $\mathbb{Z}_{\pi/2} = \{0, \pi/2, \pi, 3\pi/2\}$ depicted in Fig. 1 outputting the quantum state $|+_\theta\rangle$ on its right interface, and the classical description of this state, θ, on its left interface.

In Section 3, we show a wide-ranging limitation to the universally composable guarantees that any protocol in the family $\mathsf{RSP}_{\mathsf{CC}}$ can achieve. The limitation follows just from the relation between (i) the notion of classical realization and (ii) a property we call describability – which roughly speaking measures how leaky an RSP resource is, i.e. what amount of information about the classical description of the final state can be extracted by an unbounded malicious server. We emphasize that even if this specific property is an information-theoretic notion, our final impossibility result also targets computational security. The limitation directly affects the amount of additional leakage on the classical description of the quantum state. In this way, it rules out a wide set of desirable resources, even against computationally bounded distinguishers.

Theorem 1 (Security Limitations of $\mathsf{RSP}_{\mathsf{CC}}$). *Any* RSP *resource, realizable by an* $\mathsf{RSP}_{\mathsf{CC}}$ *protocol with security against quantum polynomial-time distinguishers, must leak an encoded, but complete description of the generated quantum state to the server.*

The importance of Theorem 1 lies in the fact that it is drawing a connection between the composability of an $\mathsf{RSP}_{\mathsf{CC}}$ protocol – a *computational* notion – with

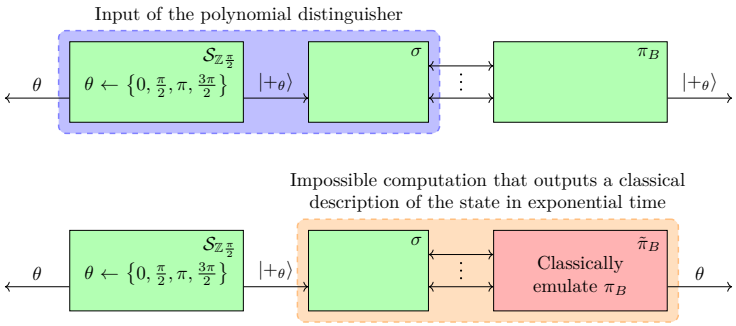


Fig. 2: Idea of the proof of impossibility of composable $\mathsf{RSP}_{\mathsf{CC}}$, exemplified by the $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$ primitive from Fig. 1. $\tilde{\pi}_B$ runs the same computations as π_B by emulating it. In this way, the classical description of the quantum state can be extracted.

the statistical leakage of the ideal functionality it is constructing – an *information-theoretic* notion. This allows us to use fundamental physical principles such as no-cloning or no-signaling in the security analysis of *computationally* secure $\mathsf{RSP}_{\mathsf{CC}}$ protocols. As one direct application of this powerful tool, we show that secure implementations of the ideal resource in Fig. 1 give rise to the construction of a quantum cloner, and are hence impossible.

Proof sketch. While Theorem 1 applies to much more general RSP resources having arbitrary behavior at its interfaces and targeting any output quantum state, for simplicity we exemplify the main ideas of our proof for the ideal resource $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$. The composable security of a protocol realizing $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$ implies, by definition, the existence of a simulator σ which turns the right interface of the ideal resource into a completely classical interface as depicted in Fig. 2. Running the protocol of the honest server with access to this classical interface allows the distinguisher to reconstruct the quantum state $|+_\theta\rangle$ the simulator received from the ideal resource. Since the distinguisher also has access to θ via the left interface of the ideal resource, it can perform a simple measurement to verify the consistency of the state obtained after interacting with the simulator. By the correctness of the protocol, the obtained quantum state $|+_\theta\rangle$ must therefore indeed comply with θ. We emphasize that this consistency check can be performed efficiently, i.e. by *polynomially-bounded* quantum distinguishers.

Since the quantum state, $|+_\theta\rangle$, is transmitted from σ to the distinguisher over a classical channel, the ensemble of exchanged classical messages must contain a complete encoding of the description of the state, θ. A (possibly computationally unbounded) algorithm can hence extract the actual description of the state using a classical emulation of the honest server. This property of the ideal resource is central to our proof technique, we call it *describability*. □

Having a full description of the quantum state produced by $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$ would allow us to clone it, a procedure prohibited by the no-cloning theorem. We conclude that the resource $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$ cannot be constructed from a classical channel only.

One could attempt to modify the ideal resource, to incorporate such an extensive leakage, which is necessary as the above proof implies. However, this yields an ideal resource that is not a useful idealization or abstraction of the real world (because it is fully leaky, i.e. reveals to a malicious server the full classical description of the state) which puts in question whether they are at all useful in a composable analysis. Indeed, ideal resources are typically described in a way that it is obvious that they are secure (i.e. in a perfect, ideal sense), and we can then claim that a protocol is secure because it is (for any computationally bounded distinguisher) indistinguishable from the perfectly secure resource. Consider for example constructions of composite protocols that utilize a (non-leaky) ideal resource as a sub-module, say that leaks only the size of an encrypted message. These constructions require a fresh security analysis if the sub-module is replaced by any leaky version of it (like a resource leaking a specific encrypted form of the real message), but since the modified resource is very specific and not trivially secure, it appears that this replacement does not give any benefit compared to directly using the implementation as a subroutine and then examining the composable security of the combined protocol as a whole. This latter way is therefore examined next.

More precisely, we might still be able to use $\mathsf{RSP}_{\mathsf{CC}}$ protocols as a subroutine in other, specific protocols, and expect the overall protocol to still construct a useful ideal functionality. The protocol family $\mathsf{UBQC}_{\mathsf{CC}}$ is such an application. Unfortunately, as we show in Section 4, $\mathsf{UBQC}_{\mathsf{CC}}$ fails to provide the expected composable security guarantees once classical remote state preparation is used to replace the quantum channel from client to server (where composable security for UBQC refers to the goal of achieving the established ideal functionality of [DFPR14] which we recall in Section 4). This holds even if the distinguisher is computationally bounded.

Theorem 3 (Impossibility of $\mathsf{UBQC}_{\mathsf{CC}}$). *No* $\mathsf{RSP}_{\mathsf{CC}}$ *protocol can replace the quantum channel in the* UBQC *protocol while preserving composable security.*

Proof sketch. To prove the impossibility of $\mathsf{UBQC}_{\mathsf{CC}}$ protocol we show that there does not exist any simulator that can be attached to the ideal UBQC functionality to emulate the behavior of concrete $\mathsf{UBQC}_{\mathsf{CC}}$ protocol. This $\mathsf{UBQC}_{\mathsf{CC}}$ uses any $\mathsf{RSP}_{\mathsf{CC}}$ protocol as a subroutine in the UBQC protocol of [BFK09] to enable the delegation of quantum computation with a completely classical-client. The proof proceeds in three steps. Firstly, we realize that the possibility of a composable $\mathsf{UBQC}_{\mathsf{CC}}$ protocol, which delegates arbitrary quantum computation, can be reduced to the possibility of any composable $\mathsf{UBQC}_{\mathsf{CC}}$ protocol that delegates single-qubit quantum computation. The latter protocol is much simpler to analyze. Next, we present a connection between the single-qubit $\mathsf{UBQC}_{\mathsf{CC}}$ and the RSP functionality. This step allows us to employ the toolbox we developed for our previous result (Theorem Theorem 1). Finally, we show that the existence of

a simulator for such an RSP functionality (that leaks the classical description, even in the form of an encoded message) would violate the no-signaling principle. Therefore, via this series of reduction, we show that the UBQC functionality, as defined in [DFPR14], cannot be realized with only a classical channel by any $\mathsf{UBQC}_{\mathsf{CC}}$ protocol of this kind (the one which uses RSP functionality to replace quantum channel in UBQC protocol). □

In Section 5, we show that the protocol family $\mathsf{RSP}_{\mathsf{CC}}$ contains protocols with reasonably restricted leakage that can be used as subroutines in specific applications resulting in combined protocols that offer a decent level of security. Specifically, we prove the blindness property of QF-UBQC, a concrete $\mathsf{UBQC}_{\mathsf{CC}}$ protocol that consists of the universal blind quantum computation (UBQC) protocol of [BFK09] and the specific LWE-based remote state preparation ($\mathsf{RSP}_{\mathsf{CC}}$) protocol from [CCKW19]. This yields the first provably secure $\mathsf{UBQC}_{\mathsf{CC}}$ protocol from standard assumptions with a classical RSP protocol as a subroutine.

Theorem 4 (Game-Based Security of QF-UBQC). *The universal blind quantum computation protocol with a classical client* $\mathsf{UBQC}_{\mathsf{CC}}$ *that combines the* $\mathsf{RSP}_{\mathsf{CC}}$ *protocol of* [CCKW19] *and the* UBQC *protocol of* [BFK09] *is blind in the game-based setting. We call this protocol* QF-UBQC*.*

The statement of Theorem 4 can be summarized as follows: No malicious (but computationally bounded) server in the QF-UBQC protocol could distinguish between two runs of the protocol performing different computations. This holds even when it is the adversary that chooses the two computations that it will be asked to distinguish. The security is achieved in the plain model, i.e., without relying on additional setup such as a measurement buffer. The protocol itself is a combination of UBQC with the QFactory protocol. For every qubit that the client would transmit to the server in the original UBQC protocol, QFactory is invoked as a subprocedure to the end of remotely preparing the respective qubit state on the server over a classical channel.

Proof sketch. By a series of games, we show that the real protocol on a single qubit is indistinguishable from a game where the adversary guesses the outcome of a hidden coin flip. We generalize this special case to the full protocol on arbitrary quantum computation with a polynomial number of qubits by induction over the size of the computation. □

1.2 Related Work

While $\mathsf{RSP}_{\mathsf{CC}}$ was first introduced in [CCKW18] (under a different terminology), (game-based) security was only proven against weak (honest-but-curious) adversaries. Security against malicious adversaries was proven for a modified protocol in [CCKW19], where a verifiable version of $\mathsf{RSP}_{\mathsf{CC}}$ was also given, but security was not proven in full generality. This protocol, called *QFactory*, is the basis of the positive results in this work. It is important to note that [CCKW19] only

shows the (game-based) security of QFactory whereas, in this work, we prove the (game-based) security of a classical-client delegated quantum computing protocol that uses QFactory as a subroutine. QFactory was also used as a sub-module by [Zha20] to design a blind quantum computing scheme with a succinct quantum client. In parallel [GV19] gave another protocol that offers a stronger notion of *verifiable* $\mathsf{RSP}_{\mathsf{CC}}$ and proved the security of their primitive in the CC framework. The security analysis, however, requires the assumption of a *measurement buffer* resource in addition to the classical channel to construct a verifiable $\mathsf{RSP}_{\mathsf{CC}}$. The ideal functionality of the measurement buffer takes from Alice a classical message x and from Bob a classical message ξ corresponding to the measurement operation along with a quantum state ρ, respectively, and outputs the measurement outcome $\xi(x, \rho)$ to both Alice and Bob. Bob also receives the post-measurement quantum state. Our result confirms that this measurement buffer resource is a strictly non-classical assumption.

In the information-theoretic setting with perfect security (leaking at most the input size), the question of secure delegation of quantum computation with a completely classical client was first considered in [MK14]. The authors showed a negative result by presenting a *scheme-dependent* impossibility proof. This was further studied in [DK16, ACGK19] which showed that such a classical delegation would have implications in computational complexity theory. To be precise, [ACGK19] conjecture that such a result is unlikely by presenting an oracle separation between BQP and the class of problems that can be classically delegated with perfect security (which is equivalent to the complexity class $\mathrm{NP}/\mathrm{poly} \cap \mathrm{coNP}/\mathrm{poly}$ as proven by [AFK87]). On the other hand, a different approach to secure delegated quantum computation with a completely classical client, without going via the route of $\mathsf{RSP}_{\mathsf{CC}}$, was also developed in [MDMF17] where the server is computationally unbounded and in [Mah18a, Bra18] with the computationally bounded server. The security was analyzed for the overall protocol (rather than using a module to replace quantum communication). It is worth noting that [MDMF17] is known to be not composable secure in the Constructive Cryptography framework [Man19].

2 Preliminaries

We assume basic familiarity with quantum computing, for a detailed introduction, see [NC00] (in this paper we only deal with finite dimensional Hilbert spaces).

2.1 The Constructive Cryptography Framework

There exists a few frameworks [BOM04, Unr04, Unr10, MR11] for general composability in the quantum world. We chose to use the Constructive Cryptography (CC) framework mostly because its abstraction levels allow having a result that is independent of any universal quantum computation model. Also, using CC is a common approach to analyze both classical as well as quantum primitives,

and their composable security guarantees in general and in related works including [DFPR14, MK13, DK16, GV19]. However, our results should be easy to port to other general composable frameworks.

The Constructive Cryptography (CC) framework (also sometimes referred to as the Abstract Cryptography (AC) framework) introduced by Maurer and Renner [MR11] is a top-down and axiomatic approach, where the desired functionality is described as an (ideal) *resource* $\mathcal{S}$ with a certain input-output behavior independent of any particular implementation scheme. A resource has some interfaces $\mathcal{I}$ corresponding to the different parties that could use the resource. In our case, we will have only two interfaces corresponding to Alice (the client) and Bob (the server), therefore $\mathcal{I} = \{A, B\}$. Resources are not just used to describe the desired functionality (such as a perfect state preparation resource), but also to model the assumed resources of a protocol (e.g., a communication channel). The second important notion is the *converter* which, for example, is used to define a protocol. Converters always have two interfaces, an inner and an outer one, and the inner interface can be connected to the interface of a resource. When we denote by $\pi_A \mathcal{R} \pi_B$ we refer to connecting the inner interfaces of π_A and π_B to the interfaces A and B of the resource $\mathcal{R}$.

To characterize the distance between two resources (and therefore the security), we use the so-called *distinguishers*. We then say that two resources $\mathcal{S}_1$ and $\mathcal{S}_2$ are indistinguishable (within ε), and denote it as $\mathcal{S}_1 \approx_\varepsilon \mathcal{S}_2$, if no distinguisher can distinguish between $\mathcal{S}_1$ and $\mathcal{S}_2$ with an advantage greater than ε. In the following, we will mostly focus on quantum polynomial-time (QPT) distinguishers.

Central to Constructive Cryptography is the notion of a secure construction of an (ideal) resource $\mathcal{S}$ from an assumed resource $\mathcal{R}$ by a protocol (specified as a pair of converters). We directly state the definition for the special case we are interested in, namely in two-party protocols between a client A and a server B, where A is always considered to be honest. The definition can therefore be simplified as follows:

Definition 1 (See [Mau11, MR11]). *Let $\mathcal{I} = \{A, B\}$ be a set of two interfaces (A being the left interface and B the right one), and let $\mathcal{R}, \mathcal{S}$ be two resources. Then, we say that for the two converters π_A, π_B, the protocol $\boldsymbol{\pi} := (\pi_A, \pi_B)$* (securely) constructs *$\mathcal{S}$ from $\mathcal{R}$ within ε, or that $\mathcal{R}$* realizes *$\mathcal{S}$ within ε if the following two conditions are satisfied:*

1. *Availability (i.e. correctness):*

$$\pi_A \mathcal{R} \pi_B \approx_\varepsilon \mathcal{S} \vdash \tag{1}$$

   (where $\vdash$ represents a filter, i.e. a trivial converter that enforces honest/correct behavior, and $A \approx_\varepsilon B$ means that no quantum polynomial-time (QPT) distinguisher can distinguish between A and B (given black-box access to A or B) with an advantage better than ε)
2. *Security: there exists $\sigma \in \Sigma$ (called a simulator) such that:*

$$\pi_A \mathcal{R} \approx_\varepsilon \mathcal{S} \sigma \tag{2}$$

We also extend this definition when ε is a function $\varepsilon : \mathbb{N} \to \mathbb{R}$: we say that $\mathcal{S}$ is ε-classically-realizable *if for any $n \in \mathbb{N}$, $\mathcal{S}$ is $\varepsilon(n)$-realizable.*

In our work, we instantiate a general model of computation to capture general quantum computations within converters which ensures that they follow the laws of quantum physics (e.g., excluding that the input-output behavior is signaling). Indeed, without such a restriction, we could not base our statements on results from quantum physics, because an arbitrary physical reality may not respect them, such as cloning of quantum states, signaling, and more. More specifically, in this work, we assume that any converter that interacts classically on its inner interface and outputs a single quantum message on its outer interface can be represented as a sequence of quantum instruments (which is a generalization of CPTP maps taking into account both quantum and classical outputs, see [DL70]) and constitutes the most general expression of allowed quantum operations. More precisely, this model takes into account interactive converters (and models the computation in sequential dependent stages). This is similar to if one would in the classical world instantiate the converter by a sequence of classical Turing machines (passing state to each other) [Gol01].

2.2 Notation

We denote by $\mathbb{Z}_{\frac{\pi}{2}}$ the set of the 4 angles $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$, and $\mathbb{Z}_{\frac{\pi}{4}} = \{0, \frac{\pi}{4}, ..., \frac{7\pi}{4}\}$ the similar set of 8 angles. If ρ is a quantum state, $[\rho]$ is the *classical* representation (as a density matrix) of this state. We also denote the quantum state $|+_\theta\rangle := \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$, where $\theta \in \mathbb{Z}_{\frac{\pi}{4}}$, and for any angle θ, $[\theta]$ will denote $[|+_\theta\rangle\langle+_\theta|]$, i.e. the classical description of the density matrix corresponding to $|+_\theta\rangle$. For a protocol $\mathcal{P} = (P_1, P_2)$ with two interacting algorithms P_1 and P_2 denoting the two participating parties, let $\langle P_1, P_2\rangle$ denote the execution of the two algorithms, exchanging messages. We use the notation $\mathcal{C}$ to denote the *classical channel* resource, that just forwards classical messages between the two parties.

3 Impossibility of Composable Classical RSP

In this section, we first define what RSP tries to achieve in terms of resources and subsequently quantify the amount of information that an ideal RSP resource must leak to the server. One would expect that, against a computationally bounded distinguisher, the resource can express clear privacy guarantees (i.e. a small amount of leakage), but we prove that it cannot be the case.

The reason is as follows: assuming that there exists a simulator making the ideal resource indistinguishable from the real protocol, we can exploit this fact to construct an algorithm that can classically describe the quantum state given by the ideal resource. It is not difficult to verify that there could exist an inefficient algorithm (i.e. with exponential run-time) that achieves such a task. We show that even a computationally bounded distinguisher can distinguish the real protocol from the ideal protocol whenever a simulator's strategy is independent of the

classical description of the quantum state. This would mean that for an RSP protocol to be composable there must exist a simulator that possesses at least a classical transcript encoding the description of a quantum state. This fact coupled with the quantum no-cloning theorem implies that the most meaningful and natural RSP resources cannot be realized from a classical channel alone. We finally conclude the section by looking at the class of imperfect (describable) RSP resources which avoid the no-go result at the price of being "fully-leaky", not standard, and having an unfortunately unclear composable security.

3.1 Remote State Preparation and Describable Resources

We first introduce, based on the standard definition in the Constructive Cryptography framework, the notion of *correctness* and *security* of a two-party protocol which constructs (realizes) a resource from a *classical* channel $\mathcal{C}$.

Definition 2 (Classically-Realizable Resource). *An ideal resource $\mathcal{S}$ is said to be* ε-classically-realizable *if it is realizable from a* classical *channel in the sense of Definition 1.*

A simple ideal prototype that captures the goal of a RSP protocol could be phrased as follows: the resource outputs a quantum state (chosen from a set of states) on one interface and a classical description of that state on the other interface to the client. For our purposes, this view is too narrow and we want to generalize this notion. For instance, a resource could accept some inputs from the client or interact with the server, and it may still be possible to use this resource to come up with a quantum state and its description. More precisely, if there is an efficient way to convert the client and server interfaces to comply with the basic prototype above, then such a resource can be understood as RSP resource, too. To make this idea formal, we need to introduce some converters that witness this:

1. A converter $\mathcal{A}$ will output, after interacting with the ideal resource, a classical description $[\rho]$ which is one of the following:
   (a) A density matrix (positive and with trace 1) corresponding to a quantum state ρ.
   (b) The null matrix, which is useful to denote the fact that we detected some deviation that should not happen in an honest run.
2. A converter $\mathcal{Q}$, whose goal is to output a quantum state ρ' as close as possible to the state ρ output by $\mathcal{A}$.
3. A converter $\mathcal{P}$, whose goal is to output a classical description $[\rho']$ of a quantum state ρ' which is close to ρ (cf. Definition 3).

An RSP must meet two central criteria:

1. Accuracy of the classical description of the obtained quantum state: We require that the quantum state ρ described by $\mathcal{A}$'s output is close to $\mathcal{Q}$'s output ρ'. This is to be understood in terms of the trace distance.

2. Purity of the obtained quantum state: Since the RSP resource aims to replace a noise-free quantum channel, it is desirable that the quantum state output by $\mathcal{Q}$ admit a high degree of purity, i.e. more formally, that $\mathrm{Tr}\left(\rho'^2\right)$ be close to one. Since ρ' is required to be close to ρ, this implies a high purity of ρ as well.

It turns out that these two conditions can be unified and equivalently captured requiring that the quantity $\mathrm{Tr}(\rho\rho')$ is close to one. A rigorous formulation of this claim and its proof is provided in the full version of this work [BCC+20].

An RSP resource (together with $\mathcal{A}$ and $\mathcal{Q}$) can also be seen as a resource whose accuracy can be easily *tested*. For example, if such a resource outputs a state ρ', instead of $|\phi\rangle$ (i.e. $[\rho] = [|\phi\rangle\langle\phi|]$), then one way to verify this behavior would be to measure ρ' by doing a projection on $|\phi\rangle$. This test would pass with probability $p_s := \langle\phi|\rho'|\phi\rangle$, and therefore if the resource outputs correct state (i.e. if $\rho' = |\phi\rangle\langle\phi|$), the test will always succeed. However, when ρ' is far from $|\phi\rangle\langle\phi|$, this test is unlikely to pass, and we will have $p_s < 1$. We can then generalize this same idea for arbitrary (eventually not pure) states by remarking that $p_s = \langle\phi|\rho'|\phi\rangle = \mathrm{Tr}(|\phi\rangle\langle\phi|\rho') = \mathrm{Tr}(\rho\rho')$. Indeed, this last expression corresponds exactly to the probability of outputting E_0 when measuring the state ρ' according to the POVM $\{E_0 := \rho, E_1 := I - \rho\}$, and since the classical description of ρ is known, it is possible to perform this POVM and test the (average) accuracy of the resource.When ρ is pure, the expression is equal to the (squared) fidelity between ρ and ρ'. This motivates the following definition, which characterizes the set of RSP resources.

Definition 3 (RSP resources). *A resource $\mathcal{S}$ is said to be ε-remote state preparation resource (or equivalently, a* remote state preparation resource *within ε with respect to converters $\mathcal{A}$ and $\mathcal{Q}$) if the following three conditions hold: (1) both converters output a single message at the outer interface, where the output $[\rho]$ of $\mathcal{A}$ is classical and is either a density matrix or the null matrix, and the output ρ' of $\mathcal{Q}$ can be any quantum state of same dimension as ρ; (2) the equation:*

$$\mathop{\mathbb{E}}_{([\rho],\rho')\leftarrow\mathcal{AS}\vdash\mathcal{Q}}\left[\,\mathrm{Tr}(\rho\rho')\,\right] \geq 1-\varepsilon \tag{3}$$

is satisfied, where the probability is taken over the randomness of $\mathcal{A}$, $\mathcal{S}$ and $\mathcal{Q}$, and finally, (3) for all the possible outputs $[\rho]$ of $([\rho],\rho') \leftarrow \mathcal{AS}\vdash\mathcal{Q}$, if we define $E_0 = \rho$, $E_1 = I - \rho$, then the POVM $\{E_0, E_1\}$ must be efficiently implementable by any distinguisher.

Describable resources. So far, we have specified that a resource qualifies as an RSP resource if, when all parties follow the protocol, we know how to compute a quantum state on the right interface and classical description of a "close" state on the other interface. A security-related question now is, if it is also possible to extract (possibly inefficiently) from the right interface a *classical* description of a quantum state that is close to the state described by the client. If we find a converter $\mathcal{P}$ doing this, we would call the (RSP) resource *describable*. The following definition captures this.

Definition 4 (Describable Resource). *Let $\mathcal{S}$ be a resource and $\mathcal{A}$ a converter outputting a single classical message $[\rho]$ on its outer interface (either equal to a density matrix or the null matrix). Then we say that $(\mathcal{S}, \mathcal{A})$ is* ε-describable *(or, equivalently, that $\mathcal{S}$ is describable within ε with respect to $\mathcal{A}$) if there exists a (possibly unbounded) converter $\mathcal{P}$ (outputting a single classical message $[\rho']$ on its outer interface representing a density matrix) such that:*

$$\mathop{\mathbb{E}}_{([\rho],[\rho'])\leftarrow\mathcal{A}\mathcal{S}\mathcal{P}}[\,\mathrm{Tr}(\rho\rho')\,] \geq 1-\varepsilon \tag{4}$$

(the expectation is taken over the randomness of $\mathcal{S}$, $\mathcal{A}$ and $\mathcal{P}$).

Reproducible converters. In the proof of our first result, we will encounter a crucial decoding step. Roughly speaking, the core of this decoding step is the ability to convert the classical interaction with a client, which can be seen as an arbitrary encoding of a quantum state, back into an explicit representation of the state prepared by the server. The ability of such a conversion can be phrased by the following definition.

Definition 5 (Reproducible Converter). *A converter π is said to be reproducible if there exists a converter $\tilde{\pi}$ such that the following holds*

$$\mathcal{C}\pi \approx_0^{\mathcal{D}^u} \mathcal{C}\tilde{\pi}\mathcal{T}, \tag{5}$$

where $\tilde{\pi}$, possibly inefficient converter, outputs only a classical message $[\rho']$ at its right interface, and $\mathcal{T}$ takes as input on its inner interface a classical description, $[\rho']$, of a quantum state ρ' and reproduces the exact same quantum state ρ'. The indistinguishability requirement is with respect to any unbounded distinguisher $D \in \mathcal{D}^u$ and the subscript "0" refers to perfect indistinguishability. Since $\mathcal{C}$ represents classical channel and is a neutral resource, the above condition can be equivalently written as $\pi \approx_0^{\mathcal{D}^u} \tilde{\pi}\mathcal{T}$. This is pictorially represented in Fig. 3.

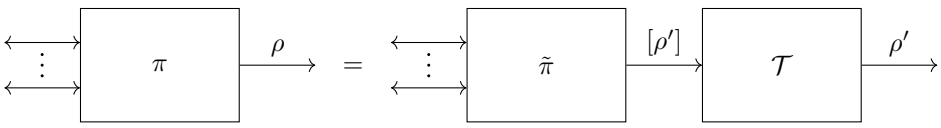


Fig. 3: Reproducible converter.

Classical communication and reproducibility. We see that in general, being reproducible is a property that stands in conflict with the quantum no-cloning theorem. More precisely, the ability to reproduce implies that there is a way to extract knowledge of a state sufficient to clone it. However, whenever communication is classical, quite the opposite is true. This is formalized in the following lemma.

Intuitively, it says that in principle it is always possible to compute the exact description of the state from the classical transcript and the *quantum instruments* (circuit) used to implement the action of the converter. The following statement is proven in the full version of this work [BCC+20].

Lemma 1. *Let $\pi = (\pi_i)_i$ be a converter, where π_i are quantum instruments corresponding to the successive rounds of the protocol π. Then π is reproducible if (i) it receives and transmits only classical messages from the inner interfaces, and (ii) it outputs at the end a quantum state on the outer interface.*

3.2 Classically-Realizable RSP are Describable

In this section we show our main result about remote state preparation resources, which interestingly links a constructive notion (*composability*) concerning a computational notion with an information-theoretic property (*describability*). As a consequence, we obtain the *impossibility* of non-describable $\mathsf{RSP}_{\mathsf{CC}}$ composable protocols (secure against *computationally bounded* distinguishers). While this connection does not rule out all the possible RSP resources, it shows that most *useful* RSP resources are impossible. Indeed, the describable property is usually not desirable, as it implies an unbounded adversary could learn the description of the state it received from an ideal resource. To illustrate this theorem, we will see in the Section 3.3 some examples showing how this result can be used to prove the impossibility of classical protocols implementing some specific resources, and in Section 3.4 we give a brief outline how "imperfect" resources could escape the impossibility result.

Theorem 1 (Classically-Realizable RSP are Describable). *If an ideal resource $\mathcal{S}$ is both an ε_1-remote state preparation with respect to some $\mathcal{A}$ and $\mathcal{Q}$ and ε_2-classically-realizable (including against only polynomially bounded distinguishers), then it is $(\varepsilon_1 + 2\varepsilon_2)$-describable with respect to $\mathcal{A}$. In particular, if $\varepsilon_1 = \mathsf{negl}(n)$ and $\varepsilon_2 = \mathsf{negl}(n)$, then $\mathcal{S}$ is describable within a negligible error $\varepsilon_1 + 2\varepsilon_2 = \mathsf{negl}(n)$.*

Proof. Let $\mathcal{S}$ be an ε_1-remote state preparation resource with respect to $(\mathcal{A}, \mathcal{Q})$ which is ε_2-classically-realizable. Then there exist π_A, π_B, σ, such that:

$$\mathop{\mathbb{E}}_{([\rho],\rho') \leftarrow \mathcal{A}\mathcal{S} \vdash \mathcal{Q}} [\operatorname{Tr}(\rho\rho')] \geq 1 - \varepsilon_1 \tag{6}$$

$$\pi_A \mathcal{C} \pi_B \approx_{\varepsilon_2} \mathcal{S} \vdash \tag{7}$$

and

$$\pi_A \mathcal{C} \approx_{\varepsilon_2} \mathcal{S}\sigma \tag{8}$$

Now, using (7), we get:

$$\mathcal{A}\pi_A \mathcal{C} \pi_B \mathcal{Q} \approx_{\varepsilon_2} \mathcal{A}\mathcal{S} \vdash \mathcal{Q} \tag{9}$$

So it means that we can't distinguish between $\mathcal{A}\mathcal{S} \vdash \mathcal{Q}$ and $\mathcal{A}\pi_A\mathcal{C}\pi_B\mathcal{Q}$ with an advantage better than ε_2 (i.e. with probability better than $\frac{1}{2}(1 + \varepsilon_2)$). But,

if we construct the following distinguisher, that runs $([\rho], \rho') \leftarrow \mathcal{AS} \vdash \mathcal{Q}$, and then measures ρ' using the POVM $\{E_0, E_1\}$ (possible because this POVM is assumed to be efficiently implementable by distinguishers in $\mathcal{D}$), with $E_0 = [\rho]$ and $E_1 = I - [\rho]$ (which is possible because we know the classical description of ρ, which is positive and smaller than I, even when $[\rho] = 0$), we will measure E_0 with probability $1 - \varepsilon_1$. So it means that by replacing $\mathcal{AS} \vdash \mathcal{Q}$ with $\mathcal{A}\pi_A\mathcal{C}\pi_B\mathcal{Q}$, the overall probability of measuring E_0 needs to be close to $1-\varepsilon_1$. More precisely, we need to have:

$$\mathop{\mathbb{E}}_{([\rho],\rho')\leftarrow\mathcal{A}\pi_A\mathcal{C}\pi_B\mathcal{Q}}[\operatorname{Tr}(\rho\rho')] \geq 1 - \varepsilon_1 - \varepsilon_2 \tag{10}$$

Indeed, if the above probability is smaller than $1 - \varepsilon_1 - \varepsilon_2$, then we can define a distinguisher that outputs 0 if it measures E_0, and 1 if it measures E_1, and his probability of distinguishing the two distributions would be equal to:

$$\frac{1}{2}\mathop{\mathbb{E}}_{([\rho],\rho')\leftarrow\mathcal{AS}\vdash\mathcal{Q}}[\operatorname{Tr}(\rho\rho')] + \frac{1}{2}\mathop{\mathbb{E}}_{([\rho],\rho')\leftarrow\mathcal{A}\pi_A\mathcal{C}\pi_B\mathcal{Q}}[\operatorname{Tr}((I-\rho)\rho')] \tag{11}$$

$$> \frac{1}{2}\left((1-\varepsilon_1) + 1 - (1-\varepsilon_1-\varepsilon_2)\right) = \frac{1}{2}(1+\varepsilon_2) \tag{12}$$

So this distinguisher would have an advantage greater than ε_2, which is in contradiction with Eq. (9).

Using a similar argument and Eq. (7), we have:

$$\mathop{\mathbb{E}}_{([\rho],\rho')\leftarrow\mathcal{AS}\sigma\pi_B\mathcal{Q}}[\operatorname{Tr}(\rho\rho')] \geq 1 - \varepsilon_1 - 2\varepsilon_2 \tag{13}$$

We will now use $\pi_B\mathcal{Q}$ to construct a $\mathcal{B}$ that can describe the state given by the ideal resource. To do that, because $\pi_B\mathcal{Q}$ interacts only classically with the inner interface and outputs a single quantum state on the outer interface, then according to Lemma 1, $\pi_B\mathcal{Q}$ is reproducible, i.e. there exists a $\mathcal{B}$ such that $\pi_B\mathcal{Q} \approx_0 \mathcal{BT}$. Note that here $\mathcal{B}$ is not efficient anymore. Of course, the proof does apply when the distinguisher is polynomially bounded. Therefore, we have:

$$\mathop{\mathbb{E}}_{([\rho],\rho')\leftarrow\mathcal{AS}\sigma\mathcal{BT}}[\operatorname{Tr}(\rho\rho')] \geq 1 - \varepsilon_1 - 2\varepsilon_2 \tag{14}$$

$\mathcal{T}$ could be omitted as it only converts the classical description $[\rho']$ into ρ'. After defining $\mathcal{P} = \sigma\mathcal{B}$, we have that $\mathcal{S}$ is $(\varepsilon_1 + 2\varepsilon_2)$-describable. □

3.3 RSP Resources Impossible to Realize Classically

In the last section, we proved that if an RSP functionality is classically-realizable (secure against polynomial quantum distinguishers), then this resource is describable by an unbounded adversary having access to the right interface of that resource.

Our main result in the previous section directly implies that as long as there exists *no unbounded* adversary that, given access to the right interface, can find the classical description given on the left interface, then the RSP resource is *impossible* to classically realize (against QPT distinguishers). Very importantly, this no-go result shows that the *only* type of RSP resources that can be classically realized are the ones that *leak* on the right interface enough information to allow a (possibly unbounded) adversary to determine the classical description given on the left interface. From a security point of view, this property is highly non-desirable, as the resource must leak the *secret description* of the state at least in *some representation*. In this section, we present some of these RSP resources that are impossible to realize classically. The proofs of all results from this section can be found in the full version of this work [BCC+20].

Definition 6 (Ideal Resource $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$). *$\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$ is the verifiable* RSP *resource (*RSP *which does not allow any deviation from the server), that receives no input, that internally picks a random $\theta \leftarrow \mathbb{Z}_{\frac{\pi}{2}}$, and that sends θ on the left interface, and $|+_\theta\rangle$ on the right interface as shown in Fig. 1.*

Lemma 2. *There exists a universal constant $\eta > 0$, such that for all $0 \leq \varepsilon < \eta$ the resource $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$ is not ε-classically-realizable.*

Next, we describe a verifiable remote state preparation RSP_V, a variant of $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$, introduced in [GV19]. Unlike $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$, in RSP_V, the dishonest server can make the resource abort and the client can partially choose the basis of the output state. However, similar to the $\mathcal{S}_{\mathbb{Z}_{\frac{\pi}{2}}}$, we prove that classically-realizable RSP_V is also not possible.

Definition 7 (Ideal Resource RSP_V, See [GV19]). *The ideal verifiable remote state preparation resource, RSP_V, takes an input $W \in \{X, Z\}$ on the left interface, but no honest input on the right interface. The right interface has a filtered functionality that corresponds to a bit $c \in \{0, 1\}$. When $c = 1$, RSP_V outputs error message* ERR *on both the interfaces, otherwise:*

1. *if $W = Z$ the resource picks a random bit b and outputs $b \in \mathbb{Z}_2$ to the left interface and a computational basis state $|b\rangle\langle b|$ to the right interface;*
2. *if $W = X$ the resource picks a random angle $\theta \in \mathbb{Z}_{\frac{\pi}{4}}$ and outputs θ to the left interface and a quantum state $|+_\theta\rangle\langle+_\theta|$ to the right interface.*

Corollary 1. *There exists a universal constant $\eta > 0$, such that for all $0 \leq \varepsilon < \eta$ the resource RSP_V is not ε-classically-realizable.*

Remark 1. Note that our impossibility of classically-realizing RSP_V does not contradict the result of [GV19]. Specifically, in their work they make use of an additional assumption of the so-called measurement buffer, see section Section 1.2. However, we show that it is impossible to realize this measurement buffer resource with a protocol interacting purely classically, therefore the measurement buffer recreates a quantum channel. Additionally, this method has a second drawback: the server can put a known state as the input of the measurement buffer, and if

the dishonest server passes the test (an event that occurs with probability $\frac{1}{n}$), then he can check that the state has not been changed, leading to polynomial security (a polynomially bounded distinguisher can distinguish between the ideal and the real world). As in CC, the security of the whole protocol is the sum of the security of the inner protocols, any protocol using this RSP as a sub-module will not be asymptotically secure (against QPT distinguisher).

3.4 Accepting the Limitations: Fully Leaky RSP resources

As explained in the previous section, Theorem 1 rules out all resources that are impossible to be *describable* with unbounded power, and that the only type of classically-realizable RSP resources would be the one leaking the full classical description of the output quantum state to an unbounded adversary, which we will refer to as being *fully-leaky* RSP. Fully-leaky RSP resources can be separated into two categories:

1. If the RSP is describable in quantum polynomial time, then the adversary can get the full description in polynomial time. This is not an interesting case as the useful properties that we know from quantum computations (such as UBQC) cannot be preserved if such a resource is employed to prepare the quantum states.
2. If the RSP is only describable using unbounded power, then these *fully-leaky* RSP resources are not trivially insecure, but their universally composable security remains unclear. Indeed, it defeats the purpose of aiming at a nice ideal resource where the provided security should be clear "by definition" and it becomes hard to quantify the impact of this additional leakage when composed with other protocols. A possible remedy would be to show restricted composition following [JM17] which we discuss in the full version of this work [BCC+20], where we also present a concrete resource that falls into this second category, i.e., one that leaks an encoding of the classical description of the final state that is not trivially decodable.

4 Impossibility of Composable Classical-Client UBQC

In the previous section, we showed that it was impossible to get a (useful) composable $\mathsf{RSP}_{\mathsf{CC}}$ protocol. A (weaker) RSP protocol, however, could still be used internally in other protocols, hoping for the overall protocol to be composably secure. To this end, we analyze the composable security of a well-known delegated quantum computing protocol, universal blind quantum computation (UBQC), proposed in [BFK09]. The UBQC protocol allows a semi-quantum client, Alice, to delegate an arbitrary quantum computation to a (universal) quantum server Bob, in such a way that her input, the quantum computation, and the output of the computation are information-theoretically hidden from Bob. The protocol requires Alice to be able to prepare single qubits of the form $|+_\theta\rangle$, where $\theta \in \mathbb{Z}\frac{\pi}{4}$ and send these states to Bob at the beginning of the protocol, the rest of the

communication between the two parties being classical. We define the family of protocols $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$ as the RSP protocols that classically delegate the preparation of an output state $|+_\theta\rangle$, where $\theta \in \mathbb{Z}\frac{\pi}{4}$. That is, without loss of generality, we assume a pair of converters P_A, P_B such that the resource $R := P_A \mathcal{C} P_B$ has the behavior of the prototype RSP resource except with negligible probability. Put differently, we assume we have an (except with negligible error) *correct* RSP protocol, but we make *no assumption about the security* of this protocol. Therefore, one can directly instantiate the quantum interaction with the $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$ at the first step as shown in Protocol 1. While UBQC allows for both quantum and classical outputs and inputs, given that we want to remove the quantum interaction in favor of a completely classical interaction, we only focus on the classical input and classical output functionality of UBQC in the remaining of the paper.

Protocol 1 UBQC with $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$ (See [BFK09])

- **Client's classical input:** An n-qubit unitary U that is represented as set of angles $\{\phi\}_{i,j}$ of a one-way quantum computation over a brickwork state/cluster state [MDF17], of the size $n \times m$, along with the dependencies X and Z obtained via flow construction [DK06].
- **Client's classical output:** The measurement outcome $\bar{s}$ corresponding to the n-qubit quantum state, where $\bar{s} = \langle 0| U |0\rangle$.

1. Client and Server runs $n \times m$ different instances of $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$ (in parallel) to obtain $\theta_{i,j}$ on client's side and $|+_{\theta_{i,j}}\rangle$ on server's side, where $\theta_{i,j} \leftarrow \mathbb{Z}\frac{\pi}{4}$, $i \in \{1, \cdots, n\}$, $j \in \{1, \cdots, m\}$
2. Server entangles all the qubits, $n \times (m-1)$ received from $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$, by applying controlled-Z gates between them in order to create a graph state $\mathcal{G}_{n \times m}$
3. For $j \in [1, m]$ and $i \in [1, n]$
   (a) Client computes $\delta_{i,j} = \phi'_{i,j} + \theta_{i,j} + r_{i,j}\pi$, $r_{i,j} \leftarrow \{0, 1\}$, where $\phi'_{i,j} = (-1)^{s^X_{i,j}} \phi_{i,j} + s^Z_{i,j}\pi$ and $s^X_{i,j}$ and $s^Z_{i,j}$ are computed using the previous measurement outcomes and the X and Z dependency sets. Client then sends the measurement angle $\delta_{i,j}$ to the Server.
   (b) Server measures the qubit $|+_{\theta_{i,j}}\rangle$ in the basis $\{|+_{\delta_{i,j}}\rangle, |-_{\delta_{i,j}}\rangle\}$ and obtains a measurement outcome $s_{i,j} \in \{0, 1\}$. Server sends the measurement result to the client.
   (c) Client computes $\bar{s}_{i,j} = s_{i,j} \oplus r_{i,j}$.
4. The measurement outcome corresponding to the last layer of the graph state ($j = m$) is the outcome of the computation.

Note that Protocol 1 is based on measurement-based model of quantum computing (MBQC). This model is known to be equivalent to the quantum circuit model (up to polynomial overhead in resources) and does not require one to perform quantum gates on their side to realize arbitrary quantum computation. Instead, the computation is performed by an (adaptive) sequence of single-qubit projective measurements that steer the information flow across a highly entangled resource state. Intuitively, UBQC can be seen as a distributed MBQC where

the measurements are performed by the server whereas the classical update of measurement bases is performed by the client. Since the projective measurements in quantum physics, in general, are probabilistic in nature and therefore, the client needs to update the measurement bases (and classically inform the server about the update) based on the outcomes of the earlier measurements to ensure the correctness of the computation. Roughly speaking, this information flow is captured by the X and Z dependencies. For more details, we refer the reader to [RB01, Nie06].

Next, we show that the Universal Blind Quantum Computing protocol [BFK09], which is proven to be secure in the Constructive Cryptography framework [DFPR14], cannot be proven composably secure (for the same ideal resource) when the quantum interaction is replaced with $\mathsf{RSP}_{\mathsf{CC}}$ (this class of protocol is denoted as $\mathsf{UBQC}_{\mathsf{CC}}$). We also give an outlook that the impossibility proof also rules out weaker ideal resources.

4.1 Impossibility of Composable $\mathsf{UBQC}_{\mathsf{CC}}$ on 1 Qubit

To prove that there exists no $\mathsf{UBQC}_{\mathsf{CC}}$ protocol, we will first focus on the simpler case when the computation is described by a single measurement angle. The resource that performs a blind quantum computation on one qubit ($\mathcal{S}_{UBQC1}$) is defined as below:

Definition 8 (Ideal resource of single-qubit UBQC (See [DFPR14])). *The definition of the ideal resource $\mathcal{S}_{UBQC1}$, depicted in Fig. 4, achieves blind quantum computation specified by a single angle ϕ. The input (ξ, ρ) is filtered when $c = 0$. The ξ can be any deviation (specified for example using the classical description of a CPTP map) that outputs a classical bit, and which can depend on the computation angle ϕ and some arbitrary quantum state ρ.*

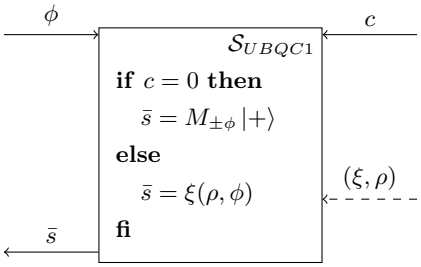


Fig. 4: Ideal resource $\mathcal{S}_{UBQC1}$ for UBQC with one angle, with a filtered (dashed) input. In the case of honest server the output $\bar{s} \in \{0, 1\}$ is computed by measuring the qubits $|+\rangle$ in the $\{|+_\phi\rangle, |-_\phi\rangle\}$ basis. On the other hand if $c = 1$ any malicious behavior of server can be captured by (ξ, ρ), i.e. the output $\bar{s}$ is computed by applying the CPTP map ξ on the input ϕ and on another auxiliary state ρ chosen by the server.

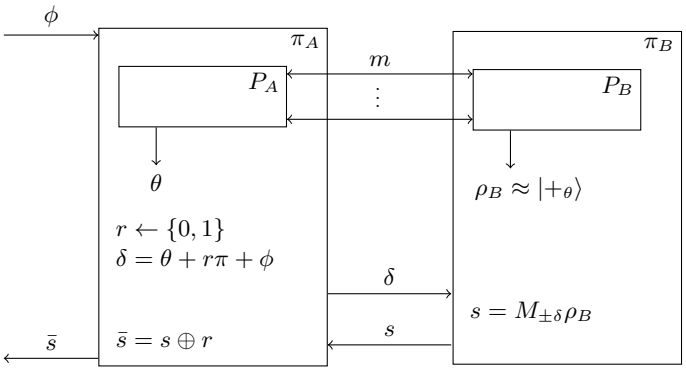


Fig. 5: UBQC with one qubit when both Alice and Bob follows the protocol honestly (see Protocol 1)

Theorem 2 (No-go composable classical-client single-qubit UBQC). *Let (P_A, P_B) be a protocol interacting only through a classical channel $\mathcal{C}$, such that $(\theta, \rho_B) \leftarrow (P_A \mathcal{C} P_B)$ with $\theta \in \mathbb{Z}_{\frac{\pi}{4}}$, and such that (by correctness) the trace distance between ρ_B and $|+_\theta\rangle\langle+_\theta|$ is negligible with overwhelming probability. Then, if we define π_A and π_B as the UBQC protocol on one qubit that makes use of (P_A, P_B) as a sub-protocol to replace the quantum channel (as pictured in Fig. 5), (π_A, π_B) is not composable, i.e. there exists no simulator σ such that:*

$$\pi_A \mathcal{C} \pi_B \approx_\varepsilon \mathcal{S}_{UBQC1} \vdash^{c=0}, \qquad \pi_A \mathcal{C} \approx_\varepsilon \mathcal{S}_{UBQC1} \sigma \tag{15}$$

for some negligible $\varepsilon = \mathsf{negl}(n)$.

Proof. In order to prove this theorem, we will proceed by contradiction. Let us assume that there exists (P_A, P_B), and a simulator σ having the above properties. Then, for the same resource $\mathcal{S}_{UBQC1}$ we consider a different protocol $\boldsymbol{\pi}' = (\pi'_A, \pi'_B)$ that realizes it, but using a different filter $\vdash^\sigma$ and a different simulator σ':

$$\pi'_A \mathcal{C} \pi'_B \approx_\varepsilon \mathcal{S}_{UBQC1} \vdash^\sigma \tag{16}$$

$$\pi'_A \mathcal{C} \approx_\varepsilon \mathcal{S}_{UBQC1} \sigma' \tag{17}$$

More specifically, the new filter $\vdash^\sigma_{UBQC1}$ will depend on σ defined in Eq. (15). Then our main proof can be described in the following steps:

1. We first show in Lemma 3 that $\mathcal{S}_{UBQC1}$ is also ε-classically-realizable by (π'_A, π'_B) with the filter $\vdash^\sigma$.
2. We then prove in Lemma 4 that the resource $\mathcal{S}_{UBQC1}$ is an RSP within $\mathsf{negl}(n)$, with respect to some well chosen converters $\mathcal{A}$ and $\mathcal{Q}$ (see Fig. 6) and this new filter $\vdash^\sigma$.
3. Then, we use the main result about RSP (Theorem 1) to show that $\mathcal{S}_{UBQC1}$ is describable within $\mathsf{negl}(n)$ with respect to $\mathcal{A}$ (Corollary 2).

4. Finally, in Lemma 6 we prove that if $\mathcal{S}_{UBQC1}$ is describable then we could achieve *superluminal signaling*, a contradiction.

The above sequence of statements concludes the proof. □

In the following, we give a brief overview of the above-mentioned statements needed to conclude Theorem 2. The proofs of these statements are given in the full version of this work [BCC+20].

Definition 9. *Let $\pi' = (\pi'_A, \pi'_B)$ the protocol realizing $\mathcal{S}_{UBQC1}$ described in the following way (as pictured Fig. 6):*

- *$\pi'_A = \pi_A$ (Fig. 5)*
- *π'_B: runs P_B, obtains a state ρ_B, then uses the angle δ received from its inner interface to compute $\tilde{\rho} := R_Z(-\delta)\rho_B$, and finally outputs $\tilde{\rho}$ on its outer interface and $s := 0$ on its inner interface.*

Then we define $\vdash^{\sigma} = \sigma\pi'_B$ depicted in Fig. 7 (with σ being the simulator from Eq. (15) above). We further let the converters $\mathcal{A}$ and $\mathcal{Q}$ be as described in Fig. 6.

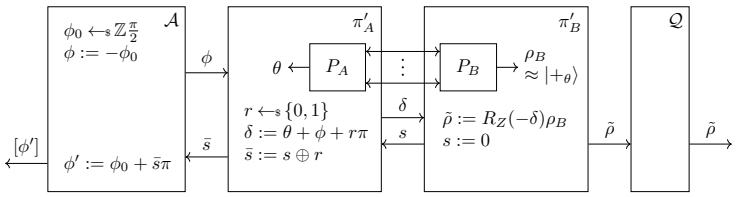


Fig. 6: Definition of $\mathcal{A}$, π'_A, π'_B and $\mathcal{Q}$.

Lemma 3. *If $\mathcal{S}_{UBQC1}$ is ε-classically-realizable by (π_A, π_B) with the filter $\vdash^{c=0}$ then $\mathcal{S}_{UBQC1}$ is also ε-classically-realizable by (π'_A, π'_B) with the filter $\vdash^{\sigma}$.*

Lemma 4. *If $\mathcal{S}_{UBQC1}$ is $\mathsf{negl}(n)$-classically-realizable with $\vdash^{c=0}$ then $\mathcal{S}_{UBQC1}$ is an $\mathsf{negl}(n)$-*remote state preparation resource *with respect the converters $\mathcal{A}$ and $\mathcal{Q}$ and filter $\vdash^{\sigma}$ defined in Fig. 6.*

Now, using our main Theorem 1 we obtain directly that if $\mathcal{S}_{UBQC1}$ is classically-realizable and RSP with respect to filter $\vdash^{\sigma}$, then it is also describable:

Corollary 2. *If $\mathcal{S}_{UBQC1}$ is $\mathsf{negl}(n)$-classically-realizable with respect to filter $\vdash^{c=0}$ then $\mathcal{S}_{UBQC1}$ is $\mathsf{negl}(n)$-describable with respect to the converter $\mathcal{A}$ described above.*

We further need a technical observation:

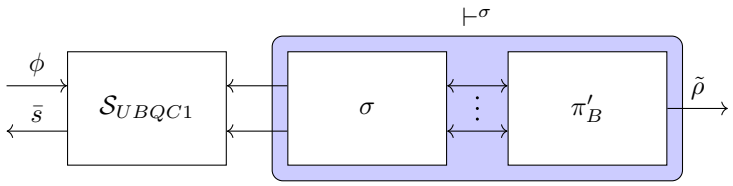


Fig. 7: Description of $\vdash^{\sigma}$

Lemma 5. *Let $\Omega = \{[\rho_i]\}$ be a set of (classical descriptions of) density matrices, such that $\forall i \neq j$, $\mathrm{Tr}(\rho_i \rho_j) \leq 1 - \eta$. Then let $([\rho], [\tilde{\rho}])$ be two random variables (representing classical description of density matrices), such that $[\rho] \in \Omega$ and $\mathop{\mathbb{E}}_{([\rho],[\tilde{\rho}])}[\,\mathrm{Tr}(\rho\tilde{\rho})\,] \geq 1-\varepsilon$, with $\eta > 6\sqrt{\varepsilon}$. Then, if we define the following "rounding" operation that rounds $\tilde{\rho}$ to the closest $\tilde{\rho}_r \in \Omega$:*

$$[\tilde{\rho}_r] := \mathrm{Round}_{\Omega}([\tilde{\rho}]) := \mathop{\arg\max}_{[\tilde{\rho}_r]\in\Omega} \mathrm{Tr}(\tilde{\rho}_r\tilde{\rho}) \tag{18}$$

Then we have:

$$\Pr_{([\rho],[\tilde{\rho}])}[\,\mathrm{Round}_{\Omega}([\tilde{\rho}]) = [\rho]\,] \geq 1 - \sqrt{\varepsilon} \tag{19}$$

In particular, if $\varepsilon = \mathsf{negl}(n)$, and $\eta \neq 0$ is a constant, $\Pr[\,\mathrm{Round}_{\Omega}([\tilde{\rho}]) = [\rho]\,] \geq 1 - \mathsf{negl}(n)$.

We state the last step of this sequence for which we give the proof here.

Lemma 6. *$\mathcal{S}_{UBQC1}$ cannot be $\mathsf{negl}(n)$-describable with respect to converter $\mathcal{A}$.*

Proof. If we assume that $\mathcal{S}_{UBQC1}$ is $\mathsf{negl}(n)$-describable, then there exists a converter $\mathcal{P}$ (outputting $[\tilde{\rho}]$) such that:

$$\mathop{\mathbb{E}}_{([\rho],[\tilde{\rho}])\leftarrow\mathcal{A}\mathcal{S}_{UBQC1}\mathcal{P}}[\,\mathrm{Tr}(\rho\tilde{\rho})\,] \geq 1 - \mathsf{negl}(n) \tag{20}$$

We define the set $\Omega := \{[|+_{\theta'}\rangle\langle+_{\theta'}|] \mid \theta' \in \{0, \pi/4, ..., 7\pi/4\}\}$. For simplicity, we will denote in the following $[\theta] = [|+_{\theta}\rangle\langle+_{\theta}|]$.

In the remaining of the proof, we are going to use the converters $\mathcal{A}$ and $\mathcal{P}$ together with the ideal resource $\mathcal{S}_{UBQC1}$, to construct a 2-party setting that would

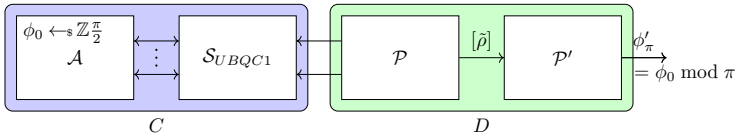


Fig. 8: Illustration of the no-signaling argument

achieve signaling, which would end our contradiction proof. More specifically, we will define a converter D running on the right interface of $\mathcal{S}_{UBQC1}$ which will manage to recover the ϕ_0 chosen randomly by $\mathcal{A}$.
As shown in Fig. 8, if we define C as $C := \mathcal{A}\mathcal{S}_{UBQC1}$ and D the converter described above, then the setting can be seen equivalently as: C chooses as random ϕ_0 and D needs to output $\phi_0 \bmod \pi$. This is however impossible, as no message is sent from $\mathcal{S}_{UBQC1}$ to its right interface (as seen in Fig. 8) (and thus no message from C to D), and therefore guessing ϕ_0 is forbidden by the no-signaling principle [GRW80].

We define $\mathcal{P}'$ as the converter that, given $[\tilde{\rho}]$ from the outer interface of $\mathcal{P}$ computes $[\tilde{\phi}] = \text{Round}_\Omega([\tilde{\rho}])$ and outputs $\tilde{\phi}_\pi = \tilde{\phi} \bmod \pi$ (as depicted in Fig. 8). We will now prove that $\tilde{\phi}_\pi = \phi_0 \bmod \pi$ with overwhelming probability.

All elements in Ω are different pure states, and in finite number, so there exist a constant $\eta > 0$ respecting the first condition of Lemma 5. Moreover from Eq. (20) we have that $\mathcal{S}_{UBQC1}$ is ε-describable with $\varepsilon = \mathsf{negl}(n)$, so we also have (for large enough n), $\eta > 6\sqrt{\varepsilon}$. Therefore, from Lemma 5, we have that:

$$\Pr_{([\rho],[\tilde{\rho}]) \leftarrow \mathcal{A}\mathcal{S}_{UBQC1}\mathcal{P}}[\,\text{Round}_\Omega([\tilde{\rho}]) = [\rho]\,] \geq 1 - \mathsf{negl}(n) \tag{21}$$

But using the definition of converter $\mathcal{A}$, we have: $[\rho] = [\phi']$, where $\phi' = \phi_0 + \bar{s}\pi$, and hence $\phi' \bmod \pi = \phi_0 \bmod \pi$. Then, using the definition of $\mathcal{P}'$, Eq. (21) is equivalent to:

$$\Pr_{([\phi'],\tilde{\phi}_\pi) \leftarrow \mathcal{A}\mathcal{S}_{UBQC1}\mathcal{P}\mathcal{P}'}[\,\tilde{\phi}_\pi = \phi_0 \bmod \pi\,] \geq 1 - \mathsf{negl}(n) \tag{22}$$

However, as pictured in Fig. 8, this can be seen as a game between $C = \mathcal{A}\mathcal{S}_{UBQC1}$ and $D = \mathcal{P}\mathcal{P}'$, where, as explained before, C picks a $\phi_0 \in \mathbb{Z}_{\frac{\pi}{2}}$ randomly, and D needs to output $\phi_0 \bmod \pi$. From Eq. (22) D wins with overwhelming probability, however, we know that since there is no information transfer from C to D, the probability of winning this game better than 1/2 (guessing the bit at random) would imply signaling. □

4.2 Impossibility of Composable $\mathsf{UBQC}_{\mathsf{CC}}$ on Any Number of Qubits

We saw in Theorem 2 that it is not possible to implement a composable classical-client UBQC protocol performing a computation on a single qubit. In this section, we prove that this result generalizes to the impossibility of $\mathsf{UBQC}_{\mathsf{CC}}$ on computations using an arbitrary number of qubits. The proof which can be found in the full version of this work [BCC+20] works by reducing the general case to the single-qubit case from the previous section.

Theorem 3 (No-go Composable Classical-Client UBQC).
Let (P_A, P_B) be a protocol interacting only through a classical channel $\mathcal{C}$, such that $(\theta, \rho_B) \leftarrow (P_A \mathcal{C} P_B)$ with $\theta \in \mathbb{Z}_{\frac{\pi}{4}}$, and such that the trace distance between ρ_B and $|+_\theta\rangle\langle+_\theta|$ is negligible with overwhelming probability. Then, if we define (π_A^G, π_B^G)

as the UBQC *protocol on any fixed graph G (with at least one output qubit, that uses (P_A, P_B) as a sub-protocol to replace the quantum channel, (π_A^G, π_B^G) is not composable, i.e. there exists no simulator σ such that:*

$$\pi_A^G \mathcal{C} \pi_B^G \approx_\varepsilon \mathcal{S}_{UBQC} \vdash^{c=0}, \qquad \pi_A^G \mathcal{C} \approx_\varepsilon \mathcal{S}_{UBQC} \sigma \tag{23}$$

for some negligible $\varepsilon = \mathsf{negl}(n)$, where $\mathcal{S}_{UBQC}$ is a trivial generalization of $\mathcal{S}_{UBQC1}$ to multiple qubits (defined in [DFPR14] under the notation $\mathcal{S}^{blind}$) for which an additional leakage l^{ψ_A} is send to the server, which is (at least in our case) equal to the size of the graph state.

5 Game-Based Security of QF-UBQC

While we know from Theorem 3 that classical-client UBQC ($\mathsf{UBQC}_{\mathsf{CC}}$) cannot be proven secure in a fully composable setting, there is hope that it remains possible with a weaker definition of security. And indeed, in this section we show that $\mathsf{UBQC}_{\mathsf{CC}}$ is possible in the *game-based setting* by implementing it using a combination of the known quantum-client UBQC Protocol 1 [BFK09] and 8-states QFactory Protocol [CCKW19]. We start with giving a formal definition of the game-based security of $\mathsf{UBQC}_{\mathsf{CC}}$.

Definition 10 (Blindness of $\mathsf{UBQC}_{\mathsf{CC}}$). *A $\mathsf{UBQC}_{\mathsf{CC}}$ protocol $\mathcal{P} = (P_C, P_S)$ is said to be (computationally) blind if no (computationally bounded) malicious server can distinguish between runs of the protocol with adversarially chosen measurement patterns on the same MBQC graph.*

In formal terms, $\mathcal{P}$ is said to be (computationally) blind if and only if for any quantum-polynomial-time adversary A it holds that

$$\Pr\left[c' = c \;\middle|\; (\phi^{(1)}, \phi^{(2)}) \leftarrow A,\, c \leftarrow_{\$} \{0,1\},\, \left\langle P_C(\phi^{(c)}), A \right\rangle,\, c' \leftarrow A\right] \leq \frac{1}{2} + \mathrm{negl}(\lambda),$$

where λ is the security parameter, and $\langle P_C(\phi^{(c)}), A\rangle$ denotes the interaction of the two algorithms $P_C(\phi^{(c)})$ and A.

Remark 2. Although, Definition 10 is written using the terminology of measurement-based model. It doesn't compromise the generality, as the model is universal and can be easily translated into a circuit model, because the measurement pattern and unitary operators are in a one-to-one mapping.

5.1 Implementing Classical-Client UBQC with QFactory

The UBQC protocol from [BFK09], where the quantum interaction is replaced by a $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$ protocol, is shown in Protocol 1. In this section, we replace the $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$ protocol with a concrete protocol proposed in [CCKW19]. This protocol, known by the name of 8-states QFactory (we consider the case where abort occurs with negligible probability) exactly emulates the capability of $\mathsf{RSP}_{\mathsf{CC}}^{8-\mathsf{states}}$. The resulting protocol contains a QFactory instance for each qubit

that would have been generated on the client's side. The keys to all QFactory instances are generated entirely independently by the client.

Unfortunately, considering the results from Section 4 there is no hope that the composable security of any $\mathsf{UBQC}_{\mathsf{CC}}$ may be achieved. Nonetheless, letting go of composability, we can prove the game-based security for this specific combination of protocols. This leads us to the main theorem of this section.

Theorem 4 (Game-based Blindness of QF-UBQC). *The protocol resulting from combining the quantum-client* UBQC *protocol with QFactory is a (computationally) blind implementation of* $\mathsf{UBQC}_{\mathsf{CC}}$ *in the game-based model according to Definition 10. We call this protocol* QF-UBQC.

The proof of Theorem 4 which will be given in the remainder of this section and follows two main ideas:

1. Every angle used in the UBQC protocol has only eight possible values, and can, therefore, be described by three bits. In the protocol, the first bit is the one for which QFactory *cannot* guarantee blindness. Fortunately, the additional one-time padding in UBQC allows analyzing the blindness of the protocol independently of the blindness of exactly this first bit. Therefore, it suffices to rely on the blindness of the last two bits which is conveniently guaranteed by QFactory and the hardness of LWE.
2. To analyze the leakage about the last two bits during a QFactory run, it is sufficient to notice that the leakage is equal to a ciphertext under an LWE-based encryption scheme. The semantic security of this encryption scheme and the hardness assumption for LWE guarantee that this leakage is negligible and can be omitted.

In more detail, the 8-states QFactory protocol which is used here consists of two combined runs of 4-states QFactory, each contributing with a single bit (hidden from the server) to the three-bit encoding of the angles used in the UBQC protocol. The formulae for how these angles from the 4-states protocol are combined in the 8-states protocol can be found in [CCKW19]. If the basis bit B_1 is the hidden bit of the first 4-states QFactory instance and basis B'_1 the hidden bit of the second instance, then we obtain:

$$L_1 = B'_2 \oplus B_2 \oplus [B_1 \cdot (s_1 \oplus s_2)],\ L_2 = B'_1 \oplus [(B_2 \oplus s_2) \cdot B_1],\ L_3 = B_1, \quad (24)$$

where $L = L_1L_2L_3 \in \{0,1\}^3$ is the description of the output state $\left|+_{L\frac{\pi}{4}}\right\rangle$, s_1, s_2 are computed by the server, and

$$B_2 = f(\mathsf{sk}, B_1, y, b), \qquad B'_2 = f(\mathsf{sk}', B'_1, y', b') \quad (25)$$

for some function f, QFactory secret keys $\mathsf{sk}, \mathsf{sk}'$, and server-chosen values y, b, y', b'.

The two 4-states QFactory instances now leak the ciphertext of B_1 and B'_1, respectively. Given the semantic security of the encryption, after a run of 8-states QFactory, L_2 and L_3 remain hidden, while the blindness of L_1 cannot be

guaranteed by QFactory. This fact is going to be crucial. Due to space constraints, we give here the security proof for the single-qubit case. By induction, the security proof can be extended to apply to UBQC for MBQC computations on a polynomial number of qubits. The proof is given in the full version of this work [BCC+20].

Lemma 7 (Blindness in the single-qubit case). *The protocol resulting from combining the quantum-client* UBQC *protocol with (8-states) QFactory is a (computationally) blind implementation of* $\mathsf{UBQC}_{\mathsf{CC}}$ *in the game-based model for MBQC computations on a single qubit.*

Proof. We start with the real protocol, describing the adaptive blindness of QFactory combined with single-qubit UBQC. In the following, we denote the set of possible angles by $M = \{j\pi/4, j = 0, \ldots, 7\}$. The encryption scheme that appears in Game 1 is the semantically secure public-key encryption scheme from [Reg09]. The two key pairs are generated independently on the challenger's side.

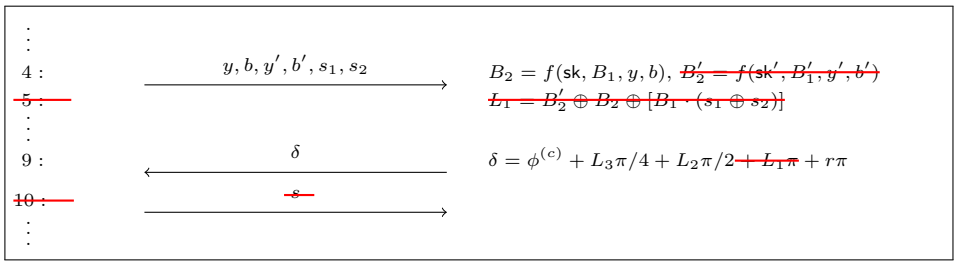
GAME 1:

	Adversary		Challenger
1 :	Choose $\phi^{(1)}, \phi^{(2)} \in M$	$\xrightarrow{\phi^{(1)}, \phi^{(2)}}$	$c \leftarrow\$ \{0,1\}$
2 :			$B_1, B_1' \leftarrow\$ \{0,1\}$
3 :		$\xleftarrow{\mathsf{pk}, \mathsf{pk}', \mathrm{Enc}^{\mathsf{pk}}(B_1), \mathrm{Enc}^{\mathsf{pk}'}(B_1')}$	Generate key pairs $(\mathsf{sk}, \mathsf{pk}), (\mathsf{sk}', \mathsf{pk}')$
4 :		$\xrightarrow{y, b, y', b', s_1, s_2}$	$B_2 = f(\mathsf{sk}, B_1, y, b),\ B_2' = f(\mathsf{sk}', B_1', y', b')$
5 :			$L_1 = B_2' \oplus B_2 \oplus [B_1 \cdot (s_1 \oplus s_2)]$
6 :			$L_2 = B_1' \oplus [(B_2 \oplus s_2) \cdot B_1]$
7 :			$L_3 = B_1$
8 :			$r \leftarrow\$ \{0,1\}$
9 :		$\xleftarrow{\delta}$	$\delta = \phi^{(c)} + L_3\pi/4 + L_2\pi/2 + L_1\pi + r\pi$
10 :		$\xrightarrow{s}$	
11 :	Compute guess $c' \in \{0,1\}$	$\xrightarrow{c'}$	Check $c' = c$?

In the following, instead of repeating the redundant parts of subsequent games, we only present incremental modifications to Game 1. Any line that is not explicitly written is assumed to be identical to the previous game.

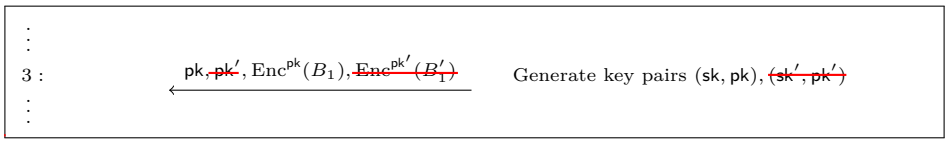
Since s is never used by the challenger, we can remove it from the protocol without distorting the success probability of the adversary. Next, we remove L_1 from the protocol and from the calculation of δ. L_1 is only used in the calculation of δ, which can be expressed as $\delta = \phi^{(c)} + L_3\pi/4 + L_2\pi/2 + (L_1 + r)\pi$. Since r is a uniform binary random variable with unique use in this line, $(L_1 + r)$ is still uniform over $\{0,1\}$ and hence removing L_1 leaves the distribution of the protocol outcome unchanged.

GAME 2:



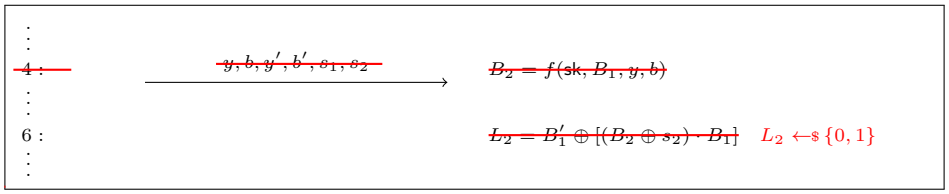
The next step introduces a (negligible) distortion to the success probability of the adversary. By the semantic security of the employed encryption scheme, no quantum-polynomial-time adversary can notice if the plaintext is replaced by pure randomness except with negligible probability, even if information about the original plaintext is leaked on the side. Therefore, replacing B_1' in the encryption by independent randomness cannot lead to a significant change in the adversary's success probability. Further, since ciphertexts of independent randomness can be equally generated by the adversary herself (having the public key), we can remove the encryption of B_1' from the protocol altogether.

GAME 3:



Next, note that B_1' perfectly one-time pads the value of L_2. This breaks the dependency of L_2 on B_2, s_2 and B_1. It does not change the distribution of L_2, if L_2 is instead directly sampled uniformly from $\{0, 1\}$. Since B_2 is unused, we remove it in the following game, and y, b, y', b', s_1, s_2 can be ignored.

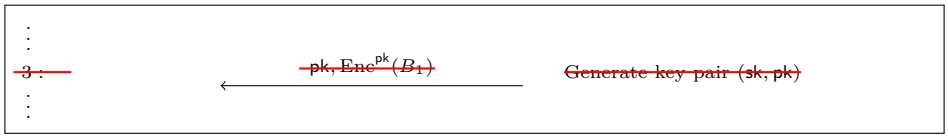
GAME 4:



By the same argument as for the transition from Game 2 to Game 3, we remove the encryption of B_1 from the following game. This introduces at most a negligible change in the success probability of the adversary.

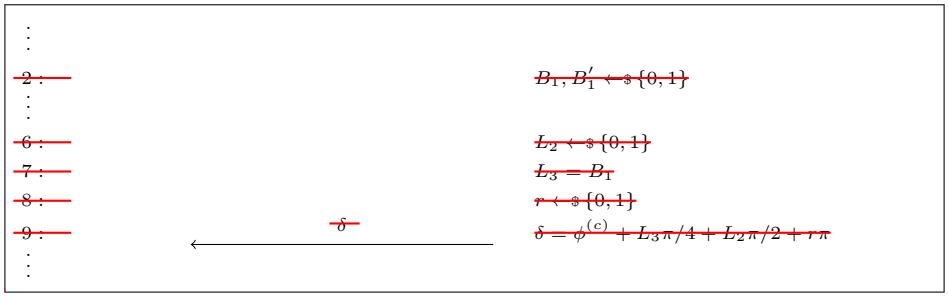
Finally, since the encryption scheme is not in use anymore, we can also remove the key generation and the message containing the public key without affecting the adversary's success probability.

GAME 5:



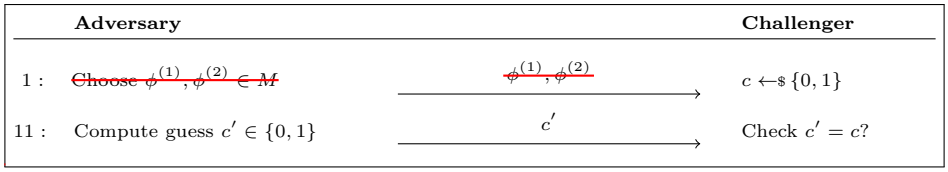
We now see that δ is a uniformly random number, L_2, L_3, and r being i.i.d. uniform bits. Therefore, the calculation and the message containing δ can be removed from the protocol without affecting the adversary.

GAME 6:



In Game 6, the inputs of the adversary are ignored by the challenger. Therefore, the computation angles $\phi^{(1)}$, $\phi^{(2)}$ can equally be removed from the protocol:

GAME 7:



Game 7 exactly describes the adversary's uninformed guess of the outcome of an independent bit flip. Therefore, by a simple information-theoretic argument, any strategy for the adversary will lead to a success probability of exactly 1/2. The proof is concluded by a standard hybrid argument [BCC+20]. □

Acknowledgments. The authors thank Céline Chevalier, Omar Fawzi, Daniel Jost, and Luka Music for very useful discussions and the anonymous reviewers of ASIACRYPT 2020 for their comments and suggestions that greatly improved this work. LC also thanks M.T. This work has been supported in part by grant FA9550-17-1-0055, by the European Union's H2020 Programme under grant agreement number ERC-669891, and by the French ANR Project ANR-18-CE39-0015 (CryptiQ). EK acknowledges support from the EPSRC Verification of Quantum Technology grant (EP/N003829/1), the EPSRC Hub in Quantum Computing and Simulation (EP/T001062/1), and the UK Quantum Technology Hub: NQIT grant (EP/M013243/1). LC and DL gratefully acknowledge support from the French ANR project ANR-18-CE47-0010 (QUDATA). LC, EK, and DL

acknowledge funding from the EU Flagship Quantum Internet Alliance (QIA) project. AM gratefully acknowledges funding from the AFOSR MURI project "Scalable Certification of Quantum Computing Devices and Networks". This work was partly done while AM was at the University of Edinburgh, UK supported by EPSRC Verification of Quantum Technology grant (EP/N003829/1).

References

ABOE08. Dorit Aharonov, Michael Ben-Or, and Elad Eban. Interactive proofs for quantum computations. *arXiv preprint arXiv:0810.5375*, 2008.

ACGK19. Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. Complexity-Theoretic Limitations on Blind Delegated Quantum Computation. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, 2019.

AFK87. Martin Abadi, Joan Feigenbaum, and Joe Kilian. On hiding information from an oracle. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 195–203. ACM, 1987.

BCC+20. Christian Badertscher, Alexandru Cojocaru, Léo Colisson, Elham Kashefi, Dominik Leichtle, Atul Mantri, and Petros Wallden. Security limitations of classical-client delegated quantum computing. Cryptology ePrint Archive, Report 2020/818, 2020. https://eprint.iacr.org/2020/818 (full version).

BFK09. Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

BJ15. Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low t-gate complexity. In *Annual Cryptology Conference*, pages 609–629. Springer, 2015.

BOM04. Michael Ben-Or and Dominic Mayers. General security definition and composability for quantum & classical protocols. *arXiv preprint quant-ph/0409062*, 2004.

Bra18. Zvika Brakerski. Quantum fhe (almost) as secure as classical. In *Annual International Cryptology Conference*, pages 67–95. Springer, 2018.

Bro15a. Anne Broadbent. Delegating private quantum computations. *Canadian Journal of Physics*, 93(9):941–946, 2015.

Bro15b. Anne Broadbent. How to verify a quantum computation. *arXiv preprint arXiv:1509.09180*, 2015.

CCKW18. Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. On the possibility of classical client blind quantum computing. *arXiv preprint arXiv:1802.08759*, 2018.

CCKW19. Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. Qfactory: Classically-instructed remote secret qubits preparation. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 615–645. Springer International Publishing, 2019.

Chi05. Andrew M Childs. Secure assisted quantum computation. *Quantum Information & Computation*, 5(6):456–466, 2005.

DFPR14. Vedran Dunjko, Joseph F Fitzsimons, Christopher Portmann, and Renato Renner. Composable security of delegated quantum computation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 406–425. Springer, 2014.

DK06. Vincent Danos and Elham Kashefi. Determinism in the one-way model. *Physical Review A*, 74(5):052310, 2006.

DK16. Vedran Dunjko and Elham Kashefi. Blind quantum computing with two almost identical states. *arXiv preprint arXiv:1604.01586*, 2016.

DKL12. Vedran Dunjko, Elham Kashefi, and Anthony Leverrier. Blind quantum computing with weak coherent pulses. *Physical Review Letters*, 108(20):200502, 2012.

DL70. E. B. Davies and J. T. Lewis. An operational approach to quantum probability. *Communications in Mathematical Physics*, 17(3):239–260, September 1970.

DSS16. Yfke Dulek, Christian Schaffner, and Florian Speelman. Quantum homomorphic encryption for polynomial-sized circuits. In *Annual Cryptology Conference*, pages 3–32. Springer, 2016.

FHM18. Joseph F Fitzsimons, Michal Hajdušek, and Tomoyuki Morimae. Post hoc verification of quantum computation. *Physical Review Letters*, 120(4):040501, 2018.

Fit17. Joseph F Fitzsimons. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(1):23, 2017.

FK17. Joseph F Fitzsimons and Elham Kashefi. Unconditionally verifiable blind quantum computation. *Physical Review A*, 96(1):012303, 2017.

GKK19. Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *Theory of computing systems*, 63(4):715–808, 2019.

Gol01. Oded Goldreich. *Foundations of Cryptography*. Cambridge University Press, Aug 2001.

GRW80. G. C. Ghirardi, Alberto Rimini, and Tullio Weber. A general argument against superluminal transmission through the quantum mechanical measurement process. *Lettere al Nuovo Cimento (1971-1985)*, 27:293–298, 1980.

GV19. Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1024–1033, 2019.

HM15. Masahito Hayashi and Tomoyuki Morimae. Verifiable measurement-only blind quantum computing with stabilizer testing. *Physical Review Letters*, 115(22):220502, 2015.

JM17. Daniel Jost and Ueli Maurer. Context-restricted indifferentiability: Generalizing UCE and implications on the soundness of hash-function constructions. *IACR Cryptol. ePrint Arch.*, 2017:461, 2017.

KMW17. Elham Kashefi, Luka Music, and Petros Wallden. The quantum cut-and-choose technique and quantum two-party computation. *arXiv preprint arXiv:1703.03754*, 2017.

KP17. Elham Kashefi and Anna Pappa. Multiparty delegated quantum computing. *Cryptography*, 1(2):12, 2017.

KW17. Elham Kashefi and Petros Wallden. Garbled quantum computation. *Cryptography*, 1(1):6, 2017.

Mah18a. Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 332–338. IEEE Computer Society, 2018.

Mah18b. Urmila Mahadev. Classical verification of quantum computations. In Mikkel Thorup, editor, *59th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2018, Paris, France, October 7-9, 2018*, pages 259–267. IEEE Computer Society, 2018.

Man19. Atul Mantri. Secure delegated quantum computing, Phd thesis, 2019.

Mau11. Ueli Maurer. Constructive cryptography–a new paradigm for security definitions and proofs. In *Theory of Security and Applications*, pages 33–56. Springer, 2011.

MDF17. Atul Mantri, Tommaso F Demarie, and Joseph F Fitzsimons. Universality of quantum computation with cluster states and (X, Y)-plane measurements. *Scientific Reports*, 7:42861, 2017.

MDMF17. Atul Mantri, Tommaso F Demarie, Nicolas C Menicucci, and Joseph F Fitzsimons. Flow ambiguity: A path towards classically driven blind quantum computation. *Physical Review X*, 7(3):031004, 2017.

MF13. Tomoyuki Morimae and Keisuke Fujii. Blind quantum computation protocol in which alice only makes measurements. *Physical Review A*, 87(5):050301, 2013.

MK13. Tomoyuki Morimae and Takeshi Koshiba. Composable security of measuring-alice blind quantum computation. *arXiv preprint arXiv:1306.2113*, 2013.

MK14. Tomoyuki Morimae and Takeshi Koshiba. Impossibility of perfectly-secure delegated quantum computing for classical client. *arXiv preprint arXiv:1407.1636*, 2014.

MR11. Ueli Maurer and Renato Renner. Abstract cryptography. In *In Innovations in Computer Science*. Citeseer, 2011.

NC00. Michael A Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

Nie06. Michael A Nielsen. Cluster-state quantum computation. *Reports on Mathematical Physics*, 57(1):147–161, 2006.

RB01. Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

Reg09. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):34, 2009.

RUV12. Ben W Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of chsh games. *arXiv preprint arXiv:1209.0448*, 2012.

TMM$^+$18. Yuki Takeuchi, Atul Mantri, Tomoyuki Morimae, Akihiro Mizutani, and Joseph F Fitzsimons. Resource-efficient verification of quantum computing using Serfling's bound. *arXiv preprint arXiv:1806.09138*, 2018.

Unr04. Dominique Unruh. Simulatable security for quantum protocols. *arXiv preprint quant-ph/0409125*, 2004.

Unr10. Dominique Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology–EUROCRYPT 2010*, pages 486–505. Springer, 2010.

Vid20. Thomas Vidick. Verifying quantum computations at scale: A cryptographic leash on quantum devices. *Bulletin of the American Mathematical Society*, 57(1):39–76, 2020.

Zha20. Jiayu Zhang. Succinct blind quantum computation using a random oracle. *ArXiv*, abs/2004.12621, 2020.